IntechOpen

An assessment of the risk of service supplier bankruptcies as a cybersecurity threat

Rebecca Parry, Nottingham Trent University, UK, rebeccca.parry@ntu.ac.uk

Abstract

Behind technology service suppliers lie companies that are subject to the risk of business failure due to market conditions and trading risks. Such failures could suddenly stop customers accessing services or content, with potentially devastating business and personal impacts, given the rising importance of digital economies. The risk can be illustrated by reference to cloud computing insolvencies but similar issues may affect other service providers. The insolvency of a cloud service provider would be likely to present problems of access to infrastructure, platforms, services and data and insolvency laws are not always designed to enable a managed closedown of a business, which would be needed to enable replacement services to be sourced and data recovered. This cybersecurity risk has barely been touched upon in literature, since it lies at the intersection between law and computer science, both areas requiring high levels of specialist understanding, and this chapter is part of initial attempts to identify the threats presented.

Keywords: Cloud computing, bankruptcy law, impact on service supply, downtime

1. Introduction

Recent years have seen increasing reliance on digital economies to support ways of working and yet the prospect of business failures in this context have not yet received detailed attention as potential cybersecurity risks. An example of a technology which is of growing significance in this environment is cloud computing, which has revolutionized professional activities, through facilitating home working as well as significantly cutting costs for businesses, financial institutions, healthcare providers and government departments. It is easy to see why cloud services have grown in popularity, as cloud computing offers significant benefits. For example, major recent usage has widely arisen in the context of home working in the wake of the Covid-19 pandemic. One way in which the cloud has been important in this context is through virtualized desktops, which can seamlessly enable an employee to work on a project both at home and in the office. Even before the pandemic, cloud computing services were increasing in importance, given their adaptability and scalability as well as other benefits, for example that software and artificial intelligence functions can be accessed more cheaply. The scalable nature of cloud services can also for example enable big data analytics to be carried out much more cheaply than was previously possible. Cloud storage also offers greater security in some ways: a lost datastick or stolen laptop no longer entails an expensive loss of

data, since the content is now securely stored in the cloud servers [1]. As a result of these and other attractions the public cloud sector has been forecast to grow by 6.3% worldwide in 2020 [2].

In spite of its considerable benefits and wide usage, the cloud computing sector is not always properly understood by those using it. Indeed, users may often not always realise that the service that they are using is provided via the cloud. Rather than consisting of anything as ethereal as storage in a cloud in the sky, as some users might envisage, cloud computing simply means that services are provided and accessed on offsite machines, rather than on a local machine. These services are operated by companies, which can get into difficulties and become insolvent and this cybersecurity risk that has barely received attention before now [3, 4].

Possible reasons why a service provider can get into difficulties include a downturn in economic conditions, mismanagement, reputational damage, hacking, terrorism and natural disasters leading to financial difficulties and insolvency. Further problems may arise if there is disruption to the services or property that the cloud service provider relies upon. A service provider which is insolvent will not be able to pay its creditors in full and bankruptcy laws provide rules to address this in a fair way, as discussed in Part 5 below. Bankruptcy proceedings are typically designed to enable creditors to be repaid efficiently and at a limited cost, yet cloud computing insolvencies present challenging difficulties of complexity from a customer perspective, since customers will want to recover their content and source alternative providers before the service is shut down. Keeping the business running while this is done will be potentially costly in a circumstance where there will be limited funds. These bankruptcies therefore present a tension between the interests of creditors, who already face the loss of most, or all, of what they are owed, and the interests of cloud computing customers who will expect that the cloud service provider continues to operate temporarily while their content is recovered.

This Chapter will first provide some background regarding cloud service provision. This will be presented in part 2, followed by a more detailed examination of the cybersecurity risk of insolvencies in this sector in part 3. Part 4 will discuss risk mitigation and then the complexities of insolvencies in this area will be discussed in Part 5. Part 6 will look at whether the law may be developed to offer more help to customers of insolvent cloud computing providers, before some conclusions are offered.

2. Concise overview of cloud service provision

The main forms of cloud service are termed IAAS, SAAS and PAAS. "IAAS" is infrastructure as a service, "SAAS" is software as a service and "PAAS" is platform as a service. IAAS primarily enables hardware provision for processing or storage, such as servers and real or virtual machines, together with virtualisation software to allocate hardware to particular customers. Examples are Rackspace and IBM Bluemix. Examples of SAAS arrangement are customers who access software such as Microsoft 365 and movies from Netflix via the cloud, rather than software on their machine. PaaS is often used for application development and deployment and an example provider is Heroku. See also Table 1, below.

Cloud services can be offered via a public cloud, a private cloud or a hybrid. Public clouds are operated by third parties for a variety of users on a pay as you go basis and hosted on the premises of the third party and, due to their nature, may be unsuitable for business critical or security sensitive information. Private clouds are operated by a single organisation for its exclusive use and are therefore low risk,

although potentially used by many employees, provided that the private cloud is hosted by the organisation on its own premises. Risks are presented where a private cloud is operated by a third party and off-premises. Hybrid clouds allow data and applications to be used across public and private clouds and commonly they will deploy the private cloud for business critical or commercially sensitive information and other data will use the public cloud. Provider failures in the cases of hybrid and public clouds and third-party provided private clouds will then give rise to problems for large numbers of users.

3. Identification of the cybersecurity risk presented by cloud computing insolvencies

It is often unappreciated by users that cloud service providers are operated by companies and they carry risks of failure, for example due to market conditions or cyber-attacks. Insolvency risks have however been identified in technology literature [5], by Lloyd's of London [6] and by research organisations [7]. Lloyd's, an insurance provider, identified the potential risk most plainly: 'reliance on a relatively small number of companies has resulted in systemic risk for businesses using their services'. Most obviously the failure of one of the leading service providers would present problems but cloud services can be provided by complex arrangements of companies and risk are presented by smaller companies also. The European Telecommunications Standards Institute considered that the bankruptcy of a cloud service provider would be 'hard to deal with'.

Yet it is clear that there is potential for a cloud service provider to become bankrupt [8]. For example, Fusion Connect Inc filed for Chapter 11 bankruptcy protection in the US in 2020. There have been other previous examples. Nirvanix filed for US Chapter 11 bankruptcy protection in 2013 and gave customers two weeks' notice before closing down [9]. Other cloud providers which have gone out of business are Megaupload and MegaCloud, and the UK example of 2e2, a data centre, which failed, leaving customers with expensive costs for the recovery of their content (around £1 million or $1.3 million) [10].

In the event of bankruptcy of a cloud service provider, a customer will be faced with the need to recover their content and to source an alternative provider of infrastructure, software or platform.

Type of Service	Example usage	Example providers	What is provided	Problem in the event of provider insolvency	Possible safeguards
Platform as a service, "PAAS"	Provision of platform e.g. for the development of software applications.	Heroku, Salesforce's Force.com	Operating system, middleware, virtualisation and hardware	Loss of platform	Contingency planning, identification of potential alternative platform supplier
Software as a service, "SAAS"	Provision of software enabling e.g. project management, collaboration, management tools and	Microsoft 365, Apple iCloud, Gmail, Basecamp, Trello, Netflix, Spotify, Dropbox	Underlying infrastructure, middleware, software application and application data	Loss of software and uploaded content. Potential loss of readability of data	Software escrow, copyright splitting, step-in rights. Contingency planning e.g. indentification of potential

	business processes				alternative providers (if any).
Infrastructure as a service, "IAAS"	Instant access to infrasctructure, useful for unpredictable or increased demand e.g. for big data analytics, complex website hosting	Rackspace, IBM Bluemix, Microsoft Azure, Amazon Web Services	Hardware provision for processing or storage, such as servers and real or virtual machines, together with virtualisation software to allocate hardware to particular customers	Loss of infrastructure	Contingency planning e.g. identification of alternative provider.

Table 1: Overview of cloud services and insolvency risks and safeguards

There may be considerable practical difficulties both in relation to recovery of content and the sourcing of an alternative provider. The recovery of large volumes of data is a slow process. It may be that an alternative service is unavailable. This may render content unreadable. It may be that the business is closed before customers can recover their content and make alternative arrangements. The insolvency office holder may require funding from customers to keep the business running while content is recovered. However, in an extreme case a business may simply shut down and content will be lost. Problems for customers can stem from difficulties not just of the cloud service provider itself - the service provider may have outsourced services to a third party which shuts down. Business arrangements such as these will add levels of complexity to the recovery of content from the cloud.

The potential difficulties for customers in recovering content from a cloud service provider insolvency will be considered in more detail in part 5 below.

4. Mitigation of the risk

The main steps that customers can take relate to diligence in selecting a cloud service provider and, where possible, the inclusion of terms in the agreement with the service provider to protect the customer's content in the event of insolvency. However, customers would also be wise to have an alternative plan in the event of a loss of content or access to software. Regular backups with a third-party provider would be one option, although not perfect, since any backup will be a snapshot of the content at the time of the most recent backup.

1) Assessment of supplier viability

Given the potential risk, what can customers do to protect themselves from the risk of cloud service provider insolvencies? Users would be wise to consider the potential long-term viability of cloud service providers before entering into a contract with them [11], in particular if the provider will be storing or processing data, or supplying access to important software. Large market players in the cloud service industry may offer greater prospects of longevity of supply but fewer prospects of a bespoke service. Not all customers will realistically be able to bargain with cloud service providers, as discussed below. However, some sectors such as

banking [12, 13] may place pre-conditions on eligibility for cloud service providers and large customers for example [14] may also have specifications for eligible suppliers.

It would be prudent as well to identify potential alternative service providers in the event that the worst happens and selected provider can no longer offer the contracted service, denying access to data or to critical software.

2) Contractual bargaining

Cloud computing customers may try to address the risks of insolvency contractually [15, 16] however there are limitations to the effectiveness of this. For many customers, service will be on standard terms that will contain no provision for insolvency [17]. Large companies may have more negotiating power. In the event that a customer can bargain to obtain contractual protection, it will be important to clarify that there is a distinction between the ownership of the cloud infrastructure and the ownership of content in the cloud, such as data, so that the data does not form part of the bankruptcy estate [18], as discussed in the next section. Other options would be to include:

1) Step-in rights: entitlements that are common in outsourcing contracts and enable control to be taken of the service provider. In the cloud computing context difficulties in exercising such powers would arise where there is shared infrastructure, staff and technology.
2) Software escrow is another approach, which can be of benefit to customers who access software via the cloud. Under such an arrangement a third party would hold the software source code under a software escrow arrangement and release it upon the occurrence of a triggering event, which could include the insolvency of the service provider [19].
3) A further example is copyright splitting [20], but this might be practicably difficult to implement in the event that there are numerous users of the software.

These approaches can potentially provide workable approaches in the event of a cloud service provider insolvency.

5. A concise overview of bankruptcy possibilities and their consequences

In the event that a cloud service provider gets into financial difficulties there are normally two main formal insolvency possibilities that can be used to address the company's inability to pay its debts. Most simply, the cloud service provider may be liquidated or it may be reorganized, both of which procedures will be explained below. It must be added, however that the procedures that apply in the event of insolvency are not international and they will vary depending on the country in which the proceedings are opened. This presents a complication in the case of cloud service providers, which may have supranational affairs. The proper venue in which to open insolvency proceedings may be unclear, although both the US and UK are jurisdictions with well-developed insolvency frameworks, and which both take fairly expansive approaches to jurisdiction to open insolvency proceedings [21, 22] and it may be that these will be favoured as venues in cases where there is some connection with the cloud service provider.

We can illustrate the main likely insolvency procedures and issues that may arise in this context by reference to those which operate in the US and UK. As noted, both of these countries have well-developed insolvency laws. However, insolvency laws in other countries may be more limited and so may the infrastructure to deal with proceedings in respect of insolvent cloud service providers, since courts may be over-burdened and lacking in specialist expertise and insolvency professionals may lack experience and sometimes integrity. Again, these factors may hamper efforts to recover content from the cloud since there may not be a vehicle to support a managed closedown of the company's affairs. Indeed, the sophistication of the US and UK systems does not guarantee this steady closure and customers may lose their cloud content, infrastructure, platform or software.

1) Liquidation

The process of liquidation is normally used to bring the affairs of an insolvent company to an end, with an impartial trustee (in the UK a liquidator) being appointed to do this according to detailed procedures set out in laws. Examples are the United States Chapter 7 and the UK Insolvency Act 1986, Part IV. This section will initially consider the United States position before briefly examining the position in the UK. Claims by customers of cloud computing services can potentially give rise to complexities in both jurisdictions that can only be briefly touched upon.

The opening of Chapter 7 liquidation proceedings, an accessible introduction to which can be found at [23], will give rise to an automatic stay under 11 United States Code § 362 (hereafter "USC") to prevent creditors from taking action to enforce their claims and this gives temporary protection to the debtor while the liquidation is carried out. This is however a time of vulnerability for customers since the trustee, when appointed, may not realise that the company operates a cloud service on which customers depend and may fail to take steps to ensure continuity of service, in particular since funds to do so may be lacking. Even where the trustee takes steps to continue service, s/he may lack specialist skills and experience to operate a cloud service business and may face a steep learning curve in relation to the business, combined with a lean staffing structure and high volume of communications from concerned customers. Moreover, liquidation is not primarily a vehicle to enable ongoing trading. In the US, the business may continue to operate if it is in "the best interest of the estate and consistent with the orderly liquidation of the estate" under 11 USC §721 and this might feasibly enable a temporary operation of the company to enable customer needs to be attended to. There is a risk however that there may be insufficient funds to enable the trustee to continue to operate the business for long enough to enable customers to recover their content and it may be necessary for customers to provide funds if this is to be done.

The main role of the trustee will be to take steps to bring the company's affairs to an end by selling the company's assets and using the proceeds to pay off creditors, as far as possible, according to a system of priorities and customers claims will be dealt with as part of this. Since the trustee is dealing with the debtor's property it will be important for customers to establish their entitlement to the content that they have uploaded, so that it is not included in the estate that the trustee will be looking to sell. Preferably the customer's ownership of content should have been agreed in any contract with the cloud service provider, although the customer's ownership of the content is likely to be implied even if the contract does not address the point.

As to the distribution of assets in the liquidation, there is a distinction to be drawn between creditors with claims to specific property, such as items covered by a lien, and those without. The former are known as secured creditors and the latter as unsecured creditors. Unsecured creditors are further divided into those with priority and nonpriority status. In view of the secured creditors' claims to specific assets, or classes of assets, these assets do not form part of the estate for distribution to creditors. Similarly, customers with ownership of the content uploaded to the cloud are entitled to recover the content, since it does not form part of the estate, but this may be more difficult in practical terms, as discussed elsewhere in this Chapter. Unsecured creditors, in contrast, typically occupy a low level of priority.

As previously noted, there are two types: priority unsecured and nonpriority unsecured. The priority claims, such as the costs of running the bankruptcy, are to be paid first, so that nonpriority claims may have limited prospects for payment. The class of nonpriority unsecured creditors would be those with claims to damages. These might include cloud service customers whose service contracts have been prematurely discontinued, or other claims to damages as a result of breaches of the service contract. These claims are unsecured and are not therefore claims to specific assets and so they do not have priority and will have a low ranking in the scheme of priority for payment, as nonpriority unsecured.

It is important to look in a little more detail at the claims that customers may have based on service agreements and how they will fare in the bankruptcy. In the liquidation these will be regarded as executory contracts [24] under 11 USC § 365(a), since both parties have ongoing performance obligations at the time of the bankruptcy filing and, as such, the trustee can choose whether or not to continue performance. If the trustee elects to discontinue performance the customer will have merely a claim to damages, which, as discussed in the previous paragraph, is likely to be worthless in the liquidation, and their access to content may be lost. Similar considerations apply in relation to software licenses that customers hold, however there are additional protections under 11 USC §365(n) for customers in this instance, since customers can elect to retain rights under the contract to the software and its embodiments, including source code. This does not however require the liquidator to perform any of the licensor's obligations, such as updating the software, which can present problems for customers unless and until a replacement provider can be found, or unless the liquidator assigns the software to a third party capable of continuing service. Nor are all cloud computing services necessarily protected by this provision, since not all will have the character of software licences, even SAAS contracts, since the customer does not necessarily obtain a copy of the software, s/he merely accesses it online.

Ongoing trading in liquidation is also potentially difficult in the UK as similar issues will arise. Under the legislation, the liquidator of a company may continue to carry on business "so far as may be necessary for its beneficial winding up", according to Insolvency Act 1986, Sch 4, para 5, but this does not guarantee that there will be ongoing trading or that any period of ongoing trading will again be long enough to enable customers to recover their content and make alternative arrangements. In addition to the practical problems noted in the US context, the liquidator is not obliged to honour customers' service agreements and the liquidator has powers under Insolvency Act 1986, s 178 to disclaim unprofitable contracts, which could include cloud service agreements. Where the customer benefits from a software license one possibility is that the liquidator will prefer to assign the software to a third party, in which case this third party will normally be subject to the license, see further [25].

2) Reorganisation

Reorganisation, on the other hand, is designed to enable ongoing trading, through the restructuring of the debtor's financial obligations. Notable examples are the US Chapter 11 and the UK administration. There are great variations in reorganization laws globally and some jurisdictions as yet lack viable procedures. The main objective of reorganization proceedings is to enable struggling but viable companies to recover from their difficulties, although these procedures are not always used to achieved this. Often reorganization is used to enable the sale of the company's underlying business, prior to a liquidation of the company, or to otherwise enable greater returns to be made to creditors in liquidation.

Taking the US Chapter 11 as a well-developed system of reorganization proceedings, the company's management will become what is termed a "debtor in possession", under 11 USC §1101(1), unless a trustee is appointed. Briefly, this means that the company's pre-Chapter 11 management will remain in control, with or without personnel changes. The debtor in possession will formulate a plan of reorganization, which must be approved by creditors and by the court, and this can enable the debtor to continue trading. The debtor in possession has the power to reject contracts, as discussed in relation to liquidation. A valuable feature of Chapter 11, which also applies in Chapter 7, is the automatic stay in 11 USC § 362 and this will protect the cloud service provider from debt collection efforts by creditors, including lawsuits. Chapter 11 therefore may offer better prospects of continue trading but it is also a relatively expensive process that is used in only a small minority of insolvencies in the US.

A new UK procedure, the restructuring plan, is similar to Chapter 11 and would be suitable for larger companies which have viable prospects of recovery from their difficulties. In the UK there is also a more simple option, the company voluntary arrangement in Insolvency Act 1986, Part 1, which enables a company to reach agreement with creditors or members and does not need to be presented to a court for approval. However, the company voluntary arrangement does not provide the company with a moratorium/automatic stay on creditor claims.

Moratorium protection can be obtained if the company is first put into administration under Insolvency Act 1986, Sch B1, whether or not the plan is to introduce a company voluntary arrangement or restructuring plan. This is a relatively expensive procedure where an administrator is appointed by the company or a major creditor to take control of the company in circumstances where the company can't pay its debts, or where it is reasonably likely to become unable to pay its debts. Administration, as it was originally designed, can be used to manage the company with a view to presenting to creditors proposals for how the company can be saved, however it is more often used to achieve greater returns to creditors than would be possible in an immediate liquidation. Administration is not particularly well suited to a managed closedown of a cloud service provider since an appointment must be reasonably likely to achieve the purpose of administration, set out in Insolvency Act 1986, Sch B1, para 3. The primary purpose of administration is to save the company but if this is not reasonably practicable efforts can be focused on achieving a better return for creditors than would be likely if it was closed down without first going into administration, or if that is not reasonably practicable to make a distribution to one or more secured or preferential creditors. Since the managed closedown of a cloud service provider would be likely to add costs without benefit to creditors it is this latter objective that would need to be relied on but there is a difficulty that the administrator must 'perform his functions in the interests of the company's creditors as a whole' and the costs of a managed closedown may reduce the sums available for creditors.

Protection can alternatively be obtained via a new procedure, the restructuring moratorium, under Insolvency Act 1986, Part 1A, which offers a cheaper option than administration but potentially a shorter duration of protection. The restructuring moratorium was introduced as part of package of reforms in the wake of the Covid-19 crisis. It enables an eligible company to enjoy the benefit of a holiday from creditor claims while under the supervision of a monitor. The protection offered will be relatively brief, lasting for an initial 20 business days, although this period can be extended. Under the process for obtaining a moratorium where the cloud service provider is not subject to a winding up petition the directors are required to file documents that indicate that the company is insolvent or approaching insolvency and that the company has likely prospects of being rescued as a going concern. It is this latter requirement that would prevent this route being used for a managed closedown of a cloud service provider. A cloud service provider which is subject to a winding up petition will only be able to obtain a moratorium following an order from the court in circumstances where this will provide a better result for the company's creditors as a whole than would be possible if the company were to be wound up without an initial period of moratorium protection. Since a managed closedown primarily is required for the benefit of customers it may be difficult to argue that it would be for the benefit of creditors as a whole.

It is a weakness that there is arguably a present lack of a reorganization procedure in the UK that can be used to temporarily facilitate ongoing trading for the managed closedown of a cloud service provider, enabling customers to recover data and source alternative services [26]. None of the many UK procedures is particularly designed for this scenario, since returns to creditors are the priorities.

6. How can legislation do more assist customers of insolvent cloud service providers?

The provision of protections for users of cloud services is something that can potentially be better addressed by different jurisdictions. Digital economies can offer significant benefits and many countries, including developing countries, are building on this. A legislative framework that can provide security of data and continuity of service in the event of insolvency can support the development of such economies, as it can attract cloud service providers which can then offer confidence to customers that there will not be a sudden and catastrophic loss of services and content. A special procedure for cloud service providers, enabling a managed closedown, would be one possibility.

An example of existing provision for cloud computing insolvencies is Art 567 of the Luxembourg Code de Commerce [27]. As originally enacted this law enabled the recovery of goods entrusted to debtors upon the debtor's insolvency and in 2012 it was extended to include intangible property such as software in recognition of the growing importance of cloud computing. Such a law would not suffice in itself, since having an entitlement to recover content in the event of the insolvency of a cloud service provider is only one problem and temporary continuity of service to enable recovery of the content is also needed.

Funding to enable temporary continuity of service by an insolvent cloud service provider would be a challenge and in the longer-term consideration might be given as to whether a fund can be established to cover the running costs of a cloud service managed closedown. The fund might be created if, for example, service providers are charged a levy, although it is also notable that cloud service providers are supranational in nature and they might be able to avoid any efforts of any one

country to charge a levy, similar to the problems that countries face in taxation. Given these practical difficulties it would likely be preferred that customers should pay, although this may give rise to collective action problems, such as holdouts.

7. Conclusion

This Chapter has provided a brief introduction to a threat to cybersecurity that has as yet received only limited attention. The potential for cloud computing insolvencies is globally significant, given the rapidly rising usage and value of content that is stored in the cloud. Importance also arises from the growth of digital economies in many countries, including developing countries, and it would be desirable for domestic laws to pay attention to this matter. The Chapter has discussed in brief how insolvencies in this sector might be handled in the US and UK and has highlighted problems that would be faced by customers of insolvent cloud service providers. Even these sophisticated jurisdictions do not presently provide effective protection for cloud service customers. It is moreover doubtful that domestic insolvency procedures alone will ever be adequate to address failures in this sector, which is supranational in nature. There is arguably a need for discussion at a global level of how cloud computing insolvencies can be addressed, and how improvements can be made to the infrastructure to support this. There is also a need to identify if there are any other complex areas of supranational technology that will have potential for significant impact of insolvencies, since similar issues are likely to arise in other cases of service supply. This Chapter has focused on cloud computing as there is here a clearly identified risk of insolvency having a significant impact and a need for legislative attention to be paid. In the longer term the development of robust laws to handle cloud computing insolvencies requires collaboration between data scientists and insolvency lawyers and attention on a global scale.

Acknowledgments

I am grateful to Roger Bisson, who first brought the risk of cloud computing insolvencies to my attention and was my co-author on a longer version article, Rebecca Parry & Roger Bisson (2020): Legal approaches to management of the risk of cloud computing insolvencies, Journal of Corporate Law Studies, DOI: 10.1080/14735970.2020.1724504. I am also grateful to Adrian Walters who provided a helpful review of that article when it was at a draft stage.

Conflict of Interest

"The author declares no conflict of interest."

References

[1] Ryan P, Falvey S. Trust in the Clouds. Computer Law & Security Review 2012;28:513.

[2] Gartner. Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3% in 2020 [Internet]. 2020. Available from: https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020 [Accessed: 2020-12-07].

[3] Parry R, Bisson R. Legal approaches to management of the risk of cloud computing insolvencies. Journal of Corporate Law Studies 2020;20:421-451. DOI: 10.1080/14735970.2020.1724504.

[4] Caplan, DS. Effects of bankruptcy of a cloud services provider. [Report]. San Francisco; 2010. Available from: https://ftp.documation.com:8443/references/ABA10a/PDfs/3_3.pdf [Accessed: 2020-12-07].

[5] Brodkin J. Gartner: Seven Cloud-Computing Security Risks. InfoWorld (Internet) 2008 Jul 3. Available from: www.infoworld.com/d/securitycentral/gartner-seven-cloud-computing-security-risks853 [Accessed: 2020-12-07] .

[6] Lloyd's. Cloud Down, Impacts on the US Economy, Emerging Risk Report 2018. (Internet) 2018, Available from: https://www.lloyds.com/news-and-insight/risk-insight/library/technology/cloud-down [Accessed: 2020-12-07].

[7] European Telecommunications Standards Institute. Special Report: Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing. Sophia Antipolis Cedex, France; 2016.

[8] Morrow T, Pender K, Lee C, Faatz D. Overview of Risks, Threats, and Vulnerabilities Faced in Moving to the Cloud. [Technical Report CMU/SEI-2019-TR-004] Carnegie Mellon University; 2019), 14.

[9] Kepes B. A Nirvanix Post Mortem - Why There's No Replacement For Due Diligence. Forbes (Internet) 2013 Sep 28. Available from: https://www.forbes.com/sites/benkepes/2013/09/28/a-nirvanix-post-mortem-why-theres-no-replacement-for-due-diligence/?sh=3cba13c72556.

[10] Computer Weekly, 2e2 datacentre administrators hold customers' data to £1m ransom. Computer Weekly (Internet) 2013 Feb 8. Available from: https://www.computerweekly.com/news/2240177744/2e2-datacentre-administrators-hold-customers-data-to-1m-ransom [Accessed: 2020-12-07]

[11] Bartolini C, El Kateb, D, Le Traon, Y. et al. Cloud providers viability. Electron Markets 2018;28:53–75. DOI: 10.1007/s12525-018-0284-7

[12] Financial Conduct Authority. Guidance for Firms Outsourcing to the 'Cloud' and other Third Party IT Services. (2019). FG16/5. Available at: https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf [Accessed: 2020-12-07]

[13] European Banking Authority, Guidelines on Outsourcing Arrangements. (2019). Available at: https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf [Accessed: 2020-12-07].

[14] Geant. GN3plus Support to Clouds Terms & Conditions Requirements for Cloud Service Providers, Draft #3.2, 2.iv. Available at: https://www.geant.org/Services/Connectivity_and_network/GTS/Documents/GN3Plus_SA7_Requirements%20DRAFT.pdf [Accessed 2020-12-07]

[15] Lifshitz L, Rothchild J, editors. Cloud 3.0: Drafting and Negotiating Cloud Computing Agreements. Chicago: ABA Publishing; 2019.

[16] European Commission. Cloud Computing Contracts [Internet]. Available from: https://ec.europa.eu/info/business-economy-euro/doing-business-

eu/contract-rules/cloud-computing/cloud-computing-contracts_en [Accessed: 2020-12-07]

[17] Michels JD, Millard C, Turton F. Contracts for Clouds, Revisited: An Analysis of the Standard Contracts for 40 Cloud Computing Services (June 11, 2020). Queen Mary School of Law Legal Studies Research Paper No. 334/2020, Available at SSRN: <ssrn.com/abstract=3624712>

[18] Bartolini C, Santos C and Ullrich C. Property and the Cloud. Computer Law & Security Review 2018;34:358

[19] Tasevski I. Business Continuity in Cloud Computing [thesis]. Tilburg University; 2014, 50-51.

[20] Louwers E-J. Continuity in the Cloud: New Practical Solutions Required, an Inventory from a Dutch Perspective [Internet]. 2013. Available from: https://louwersadvocaten.nl/app/uploads/2016/08/louwers__ernst-jan_continuity_cloud.pptx.pdf [Accessed: 2020-12-07]

[21] R3. Insolvency Forum Shopping [Internet]. 2015. Available from: https://www.r3.org.uk/stream.asp?stream=true&eid=22120&node=194&checksum=D92AFA5847F6F1EBE7FEDB3476A797DC [Accessed: 2020-12-07]

[22] Green, DM, Benzija, W. Spanning the Globe: The Intended Extraterritorial Reach of the Bankruptcy Code. American Bankruptcy Institute Law Review 2002;10:85-110

[23] US Courts. Chapter 7 Bankruptcy Basics [Internet]. Available from: https://www.uscourts.gov/services-forms/bankruptcy/bankruptcy-basics/chapter-7-bankruptcy-basics [Accessed: 2020-12-07]

[24] Countryman V, Executory Contracts in Bankruptcy: Part I. (Minn.L.Rev. 1973;57: 439, 460

[25] Toutoungi A, Adams C. Intellectual Property Licenses and Insolvency [Internet]. 2020. Available from: https://www.taylorwessing.com/en/insights-and-events/insights/2020/07/intellectual-property-licences-and-insolvency [Accessed: 2020-12-07].

[26] Parry, R. An assessment of UK insolvency laws in the light of new ways of working in the era of Covid-19. International Corporate Rescue (Forthcoming)

[27] Wellens, V. New Right to Reclaim Data from Bankrupt Cloud Computing Providers. International Law Office (Internet) 2013 Jun 28. Available from: https://www.internationallawoffice.com/Newsletters/Insolvency-Restructuring/Luxembourg/NautaDutilh-Avocats-Luxembourg/New-right-to-reclaim-data-from-bankrupt-cloud-computing-providers [Accessed: 2020-12-07]